



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,055	01/22/2001	Yasuyuki Murakami	81942.0010	9202

26021 7590 06/28/2004  
HOGAN & HARTSON L.L.P.  
500 S. GRAND AVENUE  
SUITE 1900  
LOS ANGELES, CA 90071-2611

[REDACTED] EXAMINER

[REDACTED] FIELDS, COURTNEY D

[REDACTED] ART UNIT [REDACTED] PAPER NUMBER  
2137

DATE MAILED: 06/28/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

S

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/767,055	MURAKAMI, YASUYUKI <i>S</i>
	Examiner	Art Unit
	Courtney D. Fields	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on \_\_\_\_\_.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_ is/are allowed.  
 6) Claim(s) 1-27 is/are rejected.  
 7) Claim(s) \_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____.<br>_____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date 2. | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-12, 15, 17-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Takahashi et al. (U.S. Patent No. 6,332,025).

As per claims 1,5,9,20,24, and 26, Takahashi et al. discloses a secret key registration method and system for registering/issuing a secret key comprising the steps of generating a plurality of passwords based on a basic password, sending the generated passwords to a plurality of key registration agencies, and receiving its secret keys which have been encrypted based on the passwords from the key registration/issuing agencies in Figures 1,2, and 4, and Column 8, lines 21-39, Column 9, lines 32-53, 66-67, Column 10, lines 1-49, 57-67, Column 11, lines 1-5.

As per claims 2,6,10,17,21,25, and 27, Takahashi et al. discloses the claimed limitation wherein the passwords are generated at each entity based on the basic password and a plurality of different one-way functions in Column 7, lines 13-18, 42-49.

As per claims 3,7,11,18, and 22,Takahashi et al. discloses the claimed limitation wherein each of the one-way function is a one-way hash function in Column 11, lines 64-67, Column 12, lines 1-52.

As per claims 4,8,12,19, and 23, Takahashi et al. discloses the claimed limitation wherein at each entity, the respective passwords are encrypted according to a public key method and the encrypted passwords are sent to the key registration/issuing agencies in Column 7, lines 19-41, Column 10, lines 26-49.

As per claim 15, Takahashi et al. discloses the claimed limitation wherein at each key issuing agency, a secret key of each entity is issued by using divided identification information obtained by dividing identification information of each identity in Column 19, lines 49-67, Column 20, lines 1-25.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takahashi et al. in view of Garib (U.S. Patent No. 6,728,378). As per claim 9,

Art Unit: 2137

Takahashi et al. discloses the invention as substantially claimed. However, Takahashi et al. does not explicitly disclose the feature of passwords and electronic mail sent to a key issuing agency via a homepage on the Internet. As per claim 13, Garib discloses the claimed limitation wherein at each entity, the respective passwords and its electronic mail address are sent to the respective key issuing agencies via a homepage on the Internet, and at each key issuing agency, a secret key of each entity is issued by means of electronic mail in Column 11, lines 17-46, Column 12, lines 16-45.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Takahashi et al.'s software distribution system by combining Garib's secret key messaging. The combination of Takahashi et al. and Garib provides the user with an extra degree of security for messages sent to recipients' electronic mail accounts. (See Garib, Column 7, lines 48-57)

As per claim 14, Garib discloses the claimed limitation wherein at each entity, the respective passwords are sent to the respective key issuing agencies by means of electronic mail, and at each key issuing agency, a secret key of each entity is issued by means of electronic mail in Column 13, lines 26-67.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Takahashi et al.'s software distribution system by combining Garib's secret key messaging. The combination of Takahashi et al. and Garib provides the user ensuring the integrity of sent and received messages. (See Garib, Column 6, lines 30-54)

5. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Takahashi et al. in view of Matumoto et al. (U.S. Patent No. 5,016,276). As per claim 16, Takahashi et al. discloses a secret key registration method and system for registering/issuing a secret key comprising the steps of generating a plurality of passwords based on a basic password, sending the generated passwords to a plurality of key registration agencies, and receiving its secret keys which have been encrypted based on the passwords from the key registration/issuing agencies in Figures 1,2, and 4, and Column 8, lines 21-39, Column 9, lines 32-53, 66-67, Column 10, lines 1-49, 57-67, Column 11, lines 1-5. However, Takahashi et al. does not explicitly disclose the feature of transmitting information in ciphertext. As per claim 16, Matumoto et al. discloses a cryptographic communication method for transmitting information in ciphertext form comprising the steps of at the first and second entities, generating a plurality of passwords based on a basic password, sending the generated passwords to a plurality of key issuing agencies, at each key issuing agency, generating and sending secret keys of the respective first and second entities which have been encrypted based on the respective passwords, at the first entity, generating a first common key based on the secret keys of the first entity sent from the respective key issuing agencies and identification information of the second entity as a destination, at the first entity, encrypting a plaintext into a ciphertext by using the generated first common key and transmitting the ciphertext to the second entity, at the second entity, generating a second common key identical with the first common key, based on the secret identical with the first common key, based on the secret keys of the second entity sent from the

Art Unit: 2137

respective key issuing agencies and identification information of the first entity as a destination and at the second entity, decrypting the transmitted ciphertext into a plaintext by using the generated second common key in Column 3, lines 66-68, Column 4, lines 1-61, Column 12, lines 40-65.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Takahashi et al.'s software distribution system by combining Matumoto et al.'s cryptokey generation system. Matumoto et al. provides the user an acquisition of highly secret ciphertext by using a simple operation. (See Matumoto et al., Column 2, lines 34-62)

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 703-305-8293. The examiner can normally be reached on Mon - Thu 7:00 - 5:00 pm; off every Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*MS*

cdf

June 17, 2004

*Matthew Smithers*  
MATTHEW SMITHERS  
PRIMARY EXAMINER  
*Art Unit 2137*